

*Protects your  
organization better by  
controlling access to  
applications*

## Application Control

Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols.

### Enhance Control and Network Visibility

Controlling and monitoring applications on a network can seem like a daunting task due to the wide range of available applications. It is no longer an option to simply block or allow TCP and/or UDP ports since most applications do not map to individual ports. For example, controlling traffic on an HTTP or HTTPS port is futile against complex social networking sites and cloud applications.

FortiOS leverages its massive application database to identify applications and their activities while still providing a suitable and sufficient user experience, thanks to FortiASIC Content Processors (CPs), which boost CPU performance. Organizations can adopt more granular control, such as allowing logins but not chatting over selected sites. Traffic shaping may also be applied to the application traffic that is allowed. After applying control measures, continuous monitoring ensures that the measures are effective and allow for changes in application traffic patterns to be managed.

### Key Features & Benefits

Identifies and controls application traffic	Allows organization to strengthen security policies by controlling evasive application communications.
Leverages FortiGate's hardware acceleration and software optimization	Offers more security without compromising performance.
Granular control and integration with other FortiOS capabilities	Provides administrators the ability to implement the most appropriate configuration for any given organization.

### Highlights

- Superior performance using the unique FortiASIC Content Processor that offloads heavy computation from the CPU.
- Flexible implementation with robust deployment modes and granular controls.
- Excellent visibility and management tools that help administrators improve security.



## FEATURES

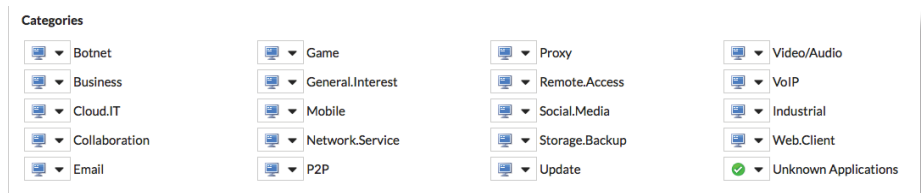
### NSS Labs “Recommend” Rating for Next Generation Firewall

Fortinet's entry into the NSS Labs Next Generation Firewall Group Test in 2013, 2014 and 2016 received the “Recommend” rating, placing it as one of the top performing systems. NSS Labs uses respectable real-world testing methodologies to measure Next Generation Firewall protection and performance, including application control.

### Superior performance with Unique Hardware Architecture

Unlike a traditional security gateway, which relies heavily on CPUs for packet inspection, the FortiGate's unique hardware architecture allows FortiOS to automatically utilize appropriate hardware components to achieve optimal performance. This prevents the CPU from becoming a bottleneck as it performs various functions concurrently.

In support of application control, the Content Processor (CP) is a specialized ASIC chip that handles demanding cryptographic computation for SSL inspection and intensive signature matching. By offloading these processes from the CPU, the FortiGate is able to minimize performance degradation when administrators opt for greater security.



### Robust Deployment Modes

FortiOS supports a wide array of network protocols and operating modes, allowing administrators to deploy the most appropriate security for their unique IT infrastructure. FortiOS also supports a variety of routing and switching protocols.

The FortiGate is able to operate in inline route and transparent mode. It can also operate in offline sniffer mode for passive monitoring of user activities. These different operating modes run concurrently by using virtual systems.

### Protection at the Edge

With today's BYOD and mobile workforce environment, it is no longer wise to deploy control just at the Internet gateway. Through Fortinet Security Fabric, FortiOS unique wireless and switch controller feature allows organizations to implement better visibility and protection closer to internal devices. Moreover, with FortiClient, administrators can also apply similar policies when mobile users are outside of the protected networks.

### Advanced Application Detection and Control

By relying on the FortiOS 3rd Generation IPS engine, the FortiGate is able to inspect many of today's encrypted and evasive traffic, as well as traffic running on new technologies, such as SPDY protocol. The inspection can be applied to both network and IPsec/SSL VPN traffic.

An application and its specific activity are identified using FortiGuard's Application Control database of over 2,500 distinct signatures. These signatures are crafted by researchers across the globe to include applications that may be unique to platforms, regions, and/or languages. It also offers specific application activity identification, such as a Facebook posting or Dropbox file sync. The database is kept up to date via scheduled or manual downloads.

The application database is classified into 20 intuitive categories for ease of use. Administrators may also create specific application

overrides that differ from the category settings. These specific applications can be filtered and selected by type of behavior, risk levels, technology type, application vendor and popularity.

Administrators may also apply advanced controls, such as setting up session TTLs for specific applications using CLI commands.

### Traffic Shaping

Organizations may better utilize bandwidth and protect critical applications by enforcing granular application usage with traffic shaping. Administrators can create various traffic shaping profiles by defining traffic priority and maximum or guaranteed bandwidth. These profiles can then be assigned to targeted applications.

### User Notification

User education is central to an effective security implementation. In response to this, FortiOS lets you provide user notification when blocking an unauthorized application. The notification appears as an HTML block page for web-based applications.

Advanced notification is possible by implementing Fortinet's browser-embedded frame. And when “off-net” users are denied

## FEATURES

access, notifications appear via FortiClient's notification pop-ups.

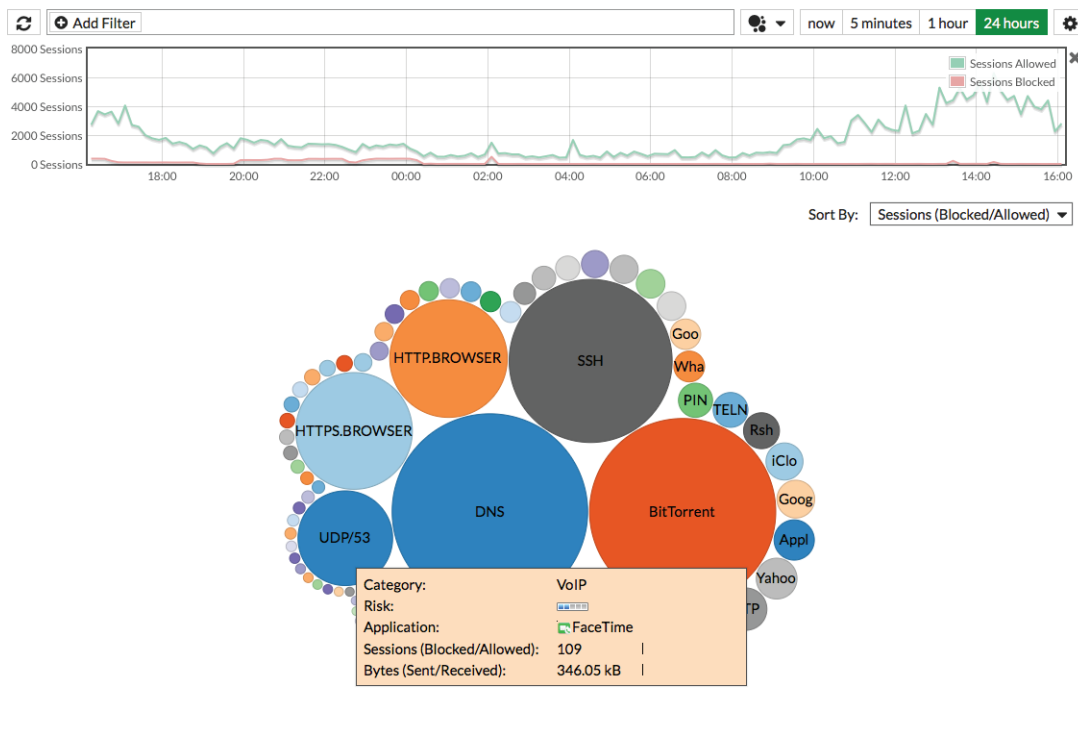
### Deep Inspection for Cloud Applications

The prevalence of cloud applications like Dropbox poses a security challenge to today's organizations. Using FortiOS's deep inspection for popular cloud applications, administrators gain deep and useful insights, via FortiView and logs, into activities associated with these applications, such as user IDs, cloud actions, file names, and file sizes. For popular video sites, FortiOS will also be able to track video files viewed.

### SSL Inspection for Encrypted Traffic

SSL (Secure Sockets Layer) is a popular encryption standard used to protect Internet traffic but may also be used to evade traditional inspection. FortiOS enables organizations to adopt effective application control even when traffic is encrypted.

Unique hardware components and software optimizations can decrypt traffic with minimal performance impact. The inspection can easily omit sensitive communications, such as financial transaction (thereby complying with privacy policies), or bypass applications that forbid SSL inspection by using granular policy settings.



## FortiGate® - End-to-end Next Generation Firewall

### Best Validated protection

FortiGate-based next generation firewall solutions are certified and validated by third-party authorities and programs such as NSS Labs, ICSA, Virus Bulletin, and AV Comparatives for superior security effectiveness.

### High Speed and Flexible Connectivity

FortiGate appliances are powered by FortiASICs and designed on purpose-built integrated architecture that provides extremely high throughput and exceptionally low latency. They also offer variety of interfaces for today's network.

### Broad Product Offerings

The FortiGate product family scales from desktop units for remote branch offices to high-end platforms for service providers and data centers while virtualized appliances support a wide range of hypervisors and public cloud infrastructure.

## FEATURES

### Monitoring, Logging, and Reporting

FortiOS empowers organization to implement security best practices that require continuous examination of threat statuses and the ability to adapt to new requirements.

The FortiView widgets provide useful analyses with detailed and contextual session information that can be filtered, ranked, and further inspected. For example, an administrator can instantly query the top applications that are currently consuming bandwidth and

drill down to identify their users and help decide if such activities should be blocked.

Network, threat, and system events activities can be archived via syslogs. In turn, these logs can generate useful trending and overview reports.

Lastly, the FortiOS offers robust in-built email and SMS alert systems. Meanwhile, integration with external threat management systems can be achieved with SNMP and standard-based syslogs.

## ADDITIONAL REFERENCE

Resource	URL
FortiOS Handbook - The Complete Guide	<a href="http://docs.fortinet.com/fortigate/admin-guides">http://docs.fortinet.com/fortigate/admin-guides</a>
Fortinet Knowledge Base	<a href="http://kb.fortinet.com/">http://kb.fortinet.com/</a>
FortiGate Product Page	<a href="https://www.fortinet.com/products-services/products/firewall.html">https://www.fortinet.com/products-services/products/firewall.html</a>



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

EMEA SALES OFFICE  
905 rue Albert Einstein  
Valbonne 06560  
Alpes-Maritimes, France  
Tel: +33.4.8987.0500

APAC SALES OFFICE  
300 Beach Road 20-01  
The Concourse  
Singapore 199555  
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
United States  
Tel: +1.954.368.9990